Available online at www.sciencedirect.com

SciVerse ScienceDirect

Procedia Engineering 15 (2011) 3376 – 3382

Procedia Engineering

www.elsevier.com/locate/procedia

Advanced in Control Engineeringand Information Science

# An Access Control Approach of Multi_Security Domain for Web Service

Song GUO[a],Xiaoping LAI[b],a*

[a]*School of Computer and Information Technology,Xinyang 464000,China*
[b]*Department of Inofromation Project,Zhao Qing Science and Technology Polytechnic,Zhaoqing 526000 ,China*

**Abstract**

Introduce several Access control approaches firstly,and analyze their disadvantages for SOA(Service-Oriented Architecture).Expatiate the advantage of the access control approach based on the attribute-trust negotiation for Web service.In this approach,the double of the trust negotiations exchange firstly the trust certificates which include several encoded attributes,then according to the policy of access control, the negotiation double exchange once and again the encryption key and reveal itself attributes step by step.This access control approach based trust negotiations make the negotiation double control displaying the attributes value of trust certificate,and have less calculating,it provides a new approach of multi_security domain for accessing safely Web service based on SOA.



Keywords:SOA;Access Control;Trust Negotiation;Web Service;Multi_Security Domain

## 1. Introduction

Web service,which discribes an interface of operational disjoint set, is based on the open criterions of WSDL,UDDI and SOAP,and so on.The request of Web service may access these operations using the criterions XML message[1],and provide the implement method for SOA.Therefore,Web service becomes the main technologe of SOA.The request usually discovery the necessary Web service by

* Corresponding author. Tel.: 13295997372.
*E-mail address*: guosong123@126.com,Laixiaoping1008@163.com.

1877-7058 © 2011 Published by Elsevier Ltd. Open access under CC BY-NC-ND license.
doi:10.1016/j.proeng.2011.08.633

UDDI[2],automatically make the program which is necessary by the request according to WSDL[3],and exchange the information with the Web service provider by SOAP[4]. Because Web service is provided by several providers, every provider is a self-government security domain, several Web services which are integrated may come from the different security domain,and they exist heterogeneity together,which make the security information from several security domain can not finish the interaction,and which will restrict accessing Web services based on SOA to some extent,the access control become one of the important security measures of accessing Web service.the Access control stipulate the restriction of object to which main body desire,on the base of the authentication, control the request of the resource provided by identity.Because SOA apply environment is distributed,the request and provider come from the different security domain, to realize the interacts each other,the double of the request and provider have to deal with the access control from several security domain,and relative to the same security domain,the access control based on SOA will be momentous challenge.

The rest of this paper is organized as following.Section 2 analyzes several access control approaches and their typical earmarks based on SOA,and expatiate their disadvantages using SOA.Section 3 depict the betterment method of access control based on attribute an auto-trust negotiation mechanism,and propose the access control method of auto-turst negotiation based on attribute ,so as to implement access control of multi-security domain for Web service based on SOA.Finally in section 4,conclusion and talk about future directions.

## 2. Frequently-used access control model

### *2.1. Identity Based Access Control*

IBAC(Identity based access control,IBAC), use the matrix based access control[3],associate authority with body identity,i.e,in the matrix, row denote the body,queue denote the object,the corresponding matrix denote the access authority of the body which associate with the object.IBAC can't satisfy the request of the distributed environment.To satisfy the applying of the distributed environment,mainly adopt two double fashion as following,the one is the centralized identity management,the another is the distributed identity alliance.

The centralized identity management use one or several authentic central servers to realize the central management to all of the body of which are participated in access control.When the body need to access Web service which is the other security domain,the central server will provide the identity certification.At present, the centralized identity management mainly include X.509 identity verification frame based access control,Kerberos[4] based access control,and the Microsoft .Net Passport[5] based access control,etc.

The distributed identity alliance does not exist the authentic central server,the different domain user each other confirm the identity using the distributed identity alliance.Before the access,several user from several domain firstly build this alliance,when the body exist in the middle of the alliance,in which Web service resource will be accessed by the body.The identity alliance of body from several domain is implemented by Web of trust.The typical distributed identity alliance include the Liberty Alliance Project(LAP), [6]and PGP access control, [7]and so on.

IBAC need some information with the identity of participators used interacting between the participators,such as the provider need the identity verification information of the request.SAML(Secure Assertion Markup Language)[8] provide the criterion of which use to pass identity verification information between the participators,the assertion is a traditional passing style of identity verification information, simultaneously,WS-Security[9] expand SOAP message, the head of SOAP include several security information,e.g., SAML assertion.

Some academicians propose the points in the distributed access control,e.g.,E.Damiani[10] advanced the access control of SOAP,which implement access control policy according to the access body identity

information, J.V.Bemmel[11] proposed access control according token, the identity of Web service request is verified during Web service discoverying,then the request verified obtain the token,and implement access control policy by the token.These researches have a common point that is implementing access control policy according to the request identity information.

SOA based application is the distributed application mode based on Web service,and Web service perhaps come from several security domains, access control policy of Web services from several security domain which lonely depend on the identity information of request is inadequate, and it restricts the application of IBAC.

### *2.2. Role Based Access Control*

RBAC(Role Based Access Control,RBAC)[12] implement authorization according to the duty function and role of body,it's principle include two mappings,the one is that maps the body to the role,when the body quest access,it will distribute a role to the body according to this mapping ;the other is that maps the role to authorization,which implement access control policy according to the role corresponding with authorization and relevant restriction rules.This management fashion is much more effective than IBAC.R.Wonoboesodo[13] will apply RBAC to Web service access control,and divide Web service into the double sort which are the single Web service and composition Web service,his basal ideology is distribute the different the role in allusion to the different Web service user,then implement the relevant authorization according to the rule.P.Liu[14] propose a RBAC of Web service which use business deal of Web service,it map the partners participating in business processing to the role,then implement the relevant authorization by the role.F.Xu[15] propose a RBAC in allusion to Web service,it map the request to one or several rules according to the request identity information,onces the request reset a role,it engenders a Actor,which symbol some relevant operation of the request.

In SOA,RBAC is applied to Web service access control, double maps mainly depend on the request body identity information. It merely depend on identity implementing mapping the body to the role as the same as IBAC.With respect to several security domain of Web service access control,because the structure of information is coarse grain,RBAC that act as an unique access control policy is distinctly insufficient.

### *2.3. Attribute Based Access Control*

ABAC(Attribute Based Access Control,ABAC) implement access control policy according to the attributes of participant entity.Attribute is some features of the body and object owning,ABAC confirm the body authorization by determining attribute conditions,sometime,which is restricted by the circumstance and system state.In unually,in ABAC,the attributes of the request body,object,and system circumstance are taken into account.W.Johnstone[16] propose the attribute based the distributed access control model,which will establish several management entities into policies,propose the request for the body attributes .When requiring to access Web service resourse, the body have to pass it's attribute certificate expressing it's attribute.N.Li propose the attribute base the conception, [17]it's idea is that depend on the body attribute information,then distribute the relevant roles.

E.Yuan[18] give attribut based Web service access control having more stranger expresss,access control policy depend on the request body attribute(such as identity,address.and so on),the attributes of resources(e.g. the server abilities of resource),and the attributes of conditions(e.g.,.load capacity).The literature[19] in allusion to the change character of circumstance attributes,propose the dynamic authorization,which dynamically adjust the relevant authorizations by the change of circumstance factors,especially.XACML(eXtensible Access Control Markup Language.XACML)[20] adequately embody the course of attribute based access control policy,PDP(Policy Decision Point.PDP) implement authorization policy depending on the attribute information of body, object and circumstance.

ABAC quietly fit the distributed circumstance such as Web service,but need attribute system to sustain.Attribute system provide the functions of attribute defining,and attribute certificate maintaining,which bring certain difficult for implementing ABAC.

## 3. Trust negotiation based Span-domain access control

In the common access control technologies, hypothesis all of the information from the same security domain,and the entity have already aforehand known,every entity in the domain realize certain action using one or several identities,system process permit or refuse them to access the given system resource information according to whether access control policy and user identity is legal.Then,in SOA,when several Web services interact with each other, several security domain establishing trust relation have made a quiet important solve,make the typical access control behave ability not equal to it's ambition when implement span-domain authourize and access control because the kinds of resource body and entities usually belong to the different management institution.Winsborough propose ATN(Automated Trust Negotiation.ATN) conception. [21]ATN is an access control method develop in the based of the traditional trust managment,which emerge the digital certificate step by step so as to establish the trust relation between the partitanters,it's main difference with trust management lie in whether aforehand acquire the other access control policy information.Comparing with the traditional access control system,the superiority of ATN as following.(1)the trust relation between the strangers is established by interacting with attribute information of particpators,and implemented by uncovering digital certificate.(2)the double of negotiations may definite the access control policy,so as to specify the other to access the sensitive resource.(3) It do not need the third(e.g.,CA) in the during of the negotiation.

### *3.1. Trust Negotiation Mode*

Trust negotiation model is the manner that the double negotiations adopt the mode of uncovering certificate and access control policy during establishing the trust relation.Winsborough advance two extreme trust negotiation model:eager stategy and parsimonious strategy. [22]the eager strategy adopt the PUSH,i.e.,before trust negotiation,the visitor like to hand in all of the certificates owning. However which result exposing some irrespective certificates and some individual privacy or the business information because handing in all of certificates and releasing certificate without any condition to the other.The parsimonious strategy adopt the PULL fashion,e.g.,the request require the certain certificate which will be provided by the visitor. The parsimonious strategy can overcome the disadvantages of protecting information of the eager strategy,but it establishing trust relation need to interact certificates time after time,the larger network expense,and the less negotiation efficiency.

### *3.2. The operational principle of automated trust negotiation*

In the automated trust negotiation model, exit several conceptions as following:

**Credential.Credential** is digital tool schlepping the relevant characters of user identity/attribute, stand for user's identity,and have the vindicability and unfalsification.It is divided into two certificates which are identity and attribute according to the purpose of different system.

**Access control policy.**Access control policy is used to protecting resource not to be accessed by the illegal user,so as to specify the legal user operating resource,the access control policy determine which certificates are announced,and by which order are announced.

**Trust negotiation strategy.**Trust negotiation strategy is the algorithm of controlling certificate announced based on access control policy.

**Trust negotiation policy.**Trust negotiation policy determine the style of trust negotiation message,which include the request of trust certificate,the answer of the request,the beginning and

termination of negotiation,the end,and the content of certification and access control stratagy message,etc.Trust negotiation policy is stored in system with the trust negotiation strategy,and is loaded down by the client.

In automated trust negotiation model,If the client tries on accessing a certain system resource by automated trust negotiation,it mainly include two steps as following:

The first phase is the fixing.If the client has not trust negotiation policy and strategy,then it must load `down them from the server in safety.

The second phrase is the execution.To access the system resource,(1)the double using trust negotiation strategy and policy exchange the attribute certificate according to access control strategy.(2)In course of automated trust negotiation,if attribute certificates sequence of the client satisfy the access cotrol strategies of the request,then they establish the trust relation each other,and the system permit the client to access the resource;otherwise,don't establish the trust relation,the request service will be refused.Resumptively, The operational principle of ATN is shown in figure 1.

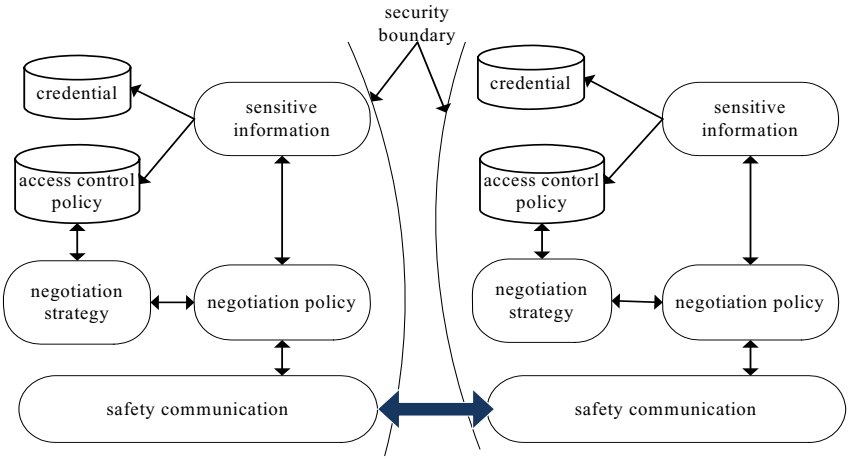


Fig. 1.The operational principle of ATN

The automated trust negotiation model can resolve access control of multi_security domain for SOA to some extent,but it also exist some disadvantages and shortcomings,e.g.,(1)The negotiation double need to exchange repeatedly trust negotiations certificates for establishing the trust relation which must bring the larger network transfers expense.At meaning time, discovering the certificate chain which is composed of the distributed digital certificate also will increase the network burden .(2) Transferring certificate over Internet which is insecure will threaten the certificate security,so the certificate security is considerably feeblish;(3)During the negotiation, the provider of resource will expose the access control strategy which is sensitive in a way,so the sensitive access control strategy will be threatened.

### *3.3. Attribute based automated trust negotiation*

In allusion to the disadvantage of the automated trust negotiation,we advance a new access control model,e.g.,the attribute based automated trust negotiation model.In open system,The trust certificate is related to the body attribute(e.g.,time,location,device sort,etc.),so establishing trust relation between the stranger entities is implemented by exchanging attributes each other.Because every entities have own of the sensitive information ,the double protect it's sensitive information by access control strategy in the course of exchange the trust certificate.

**Trust-establish-course.**The establishing trust relation firstly exchange the trust certificates comprising encryption attributes,then show itself attributes to the other by exchanging secret key step by step,and it's step as following:

(1)A send the request to B;

(2)Generating the conversation secret key Ks by the secret key algorithm between the automated trust negotiation A and B;

(3)B show its trust certificates and Web service access control strategy to A;

(4) A also show its trust certificates and Web service access control strategy to B;

(5) B show its secret key of certain attribute encrypted by conversation, and A unclose the attribute of trust certificate using the secret key of the attribute ;

(6) A show its secret key of certain attribute encrypted by conversation, and B unclose the attribute of trust certificate using the secret key of the attribute ;

Repeating the aforementioned steps,finally,whether the access control strategy satisfied determine whether A refuse the Web service provided by B.During the trust establishing, the conversation secret key is brought by the Diffie-Hellman algorithm of ellipse curve .

**Trust-negotiation-feedback.**Attribute based automated trust negotiation model,the resource is a aggregate of the sensitive information,and forbid to be accessed without authorization.At present,the resources researched which involve the sensitive information have two sorts,(1)the resource content is sensitive.Access control strategy and some attribute value of attribute certificate are sensitive,and which forbid to be accessed without authorization.(2)owning resource is sensitive:the negotiation answer and information flowing perhaps impliedly expose the fact which owns certain sensitive information.During the trust negotaition,the request answer of Web service and information flowing may reveal the sensitive information.To obtain that whether a certain body own a certain attributed the aggressor try to find the attribute certificate of the body which try to aggress，although the access control strategy protect to access the attribute,the revealing access control strategy betray the fact whether the body own the attribute. To avoid the case,we introduce the Attribute Acknowledgement Policy,for the given sensitive attribute whether is owned by the arbitrary body all is revealed the same Ack Policy, so the antagonist do not determine the body whether own the attribute from the revealed trust strategy.

## 4. Conclusion

In SOA,with more and more loose coupling of application program,if user obtain Web service from the server,they desire that the Web service provider can confirm the Web service request,verify the identity and authorization of the request,and ensure to provide the security Web service.Attribute based automated trust negotiation stand for a new the security technology,which provide the safeguard for realizing the span-domain resource sharing and accessing,have the single time exchanging the trust certificate,the less network expense,the less storing the certificates,the more effective preventing the middle attack,the higher security in comparison with the traditional automated trust negotiation .The approach provide a new idea for SOA based access control.

## Acknowledgements

Sponsored by the Natural Science foundation of Henan Province (No.102102210241,112300410197).

## References

[1] Kreger H. Web Services Conceptual Architecture 1.0, IBM Software Group. http://www.ibm.com/software/solution/webservices/pdf/WSCA.pdf,2001
[2] GUO Song,SUN XIONG-Ying.The mediation of data heterogeneity in Web services composition[C].IEEE Int'l conference on internet Technology and Applications,ITAP2010.2010.
[3] Sandhu R S, Samarati P. Access Control-Principles and Practice[J] IEEE Communication, 1994,32(9):40-48.
[4] Kohl J,Neuman C. The Kerberos Network Authentication Services. RFC1510, September 1993.
[5] Microsoft Passport Service. http://www.passport.net/.
[6] The Liberty Alliance Project. http://www.projectliberty.org/.
[7] Zimmerman P. The Qficial PGP User's Guide[M]. Cambrige: MIT Press, 1995
[8] Cantor S, Kemp J, Philpott R, et al. Assertions and Protocols for the OASIS Security Assertion Markup Language(SAML), V2.0 OASIS Standard, March 2005
[9] Nadalin A, Kaler C, et al. Web Services Security: SOAP Message Security 1.1(WS-Security 2004). OASIS Standard, February 2006
[10] Damiani E, Vimercati S D C, et al. Fine Grained Access Control for Soap E-Service[C]. WWW10, May 2001
[11] Bemmel J V, Wegdam M, et al. 3PAC:Enforcing Access Policies for Web Services[C] IEEE International Conf. on Web services(ICWS'05), 2005: 589-596
[12] Sandhu R S, et al. The NIST Model for Role based Access Control-Towards A Unified Standard[C] The 5th ACM Workshop on Role Based Access Control. July 2000
[13] Wonohoesodo R, et al. A Role-based Access Control for Web Services[C] 2004 IEEE Internaltional Conf. on Services Computing(SCC'04). 2004:49-56
[14] Liu P, Chen Z. An Access Control Model for Web Services in Business Process[C] Proceedings of the IEEE International Conf. on Web Intelligence(WI'04). 2004:292-298
[15] Xu F, Lin G, Huang H, et al. Role-based Access control System for Web Services[C] The 4th International Conf. on Computer and Information Technology(CIT'04). 2004:357-362.
[16] Johnston W, et al. Authorization and Attribute Certificates for Widely Distributed Access Control [C] IEEE Int'l Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises. 1998.
[17] Li N, Winsborough W H et al. Distributed Credential Chain Discovery in Trust Management[J]. Journal of Computer Security, 2003, 11(1):35-86.
[18] Yuan E, Tong J. Attribute-based Access Control(ABAC) for Web Service[C] IEEE International Conf. on Web Services(ICWS'05) 2005:561-569.
[19] Ryutov T. The Condition-driven Authorization Model for Distributed System Services[D] phD thsis. University of Southern California, August 2002.
[20] Moses T. eXtensible Access Control Markup Language (XACML), Version 2.0. OASIS Standard, Feb. 2005.
[21] Winsborough WH, Li NH. Towards practical automated trust negotiation. In：Michael JB. ed. Proc. of the 3rd Int'l Workshop on policies for Distributed Systems and Networks[J]. Washington: IEEE Computer Society Press, 2002: 92-103.
[22] Winsborough W H, Seamons K E, Jones VE. Automated trust negotiation. In：Hilton SC，ed. DARPA Information Survivability Conf. and Exposition MJ. New York: IEEE Press, 2000：88-102.